Quatrième Journée Normandie-Mathématiques
13 juin 2012 – INSA de Rouen

Heuristiques concernant les courbes elliptiques adaptées à la cryptographie à couplages

John BOXALL
Laboratoire de Mathématiques Nicolas Oresme

Résumé

Après quelques rappels brefs concernant la cryptogrophie à couplage et les courbes elliptiques, j'expliquerai pourquoi les courbes elliptiques adaptées à la cryptographie à couplages sont rares, et je présenterai une formule heuristique asymptotique (lorsque x tend vers l'infini) pour le nombre de classes d'isogénie de telles courbes elliptiques possédant un sous-groupe d'ordre premier d'ordre au plus x.